

Amendments to the Specification:

Please amend the specification as follows:

On Page 2, line 13:

The MN may be communicating IP data packets with a Correspondent Node (CN) which is attached to a GPRS network, then the GGSN of the GPRS network must be arranged to route the IP data packets via an appropriate bearer to the CN (which itself may be mobile). If the MN roams to a foreign network mid-session then the GGSN must be arranged to route the IP data packets to the CN (mobile user equipment) via the appropriate bearer. The appropriate bearer will have been set up by the GGSN when a session initiation was established at a time when the MN was attached to its home network. As such the parameters for the bearer will have been established with reference to a home address of the MN as the source address. However as explained above, the source address in the header of the IP data packets will be changed during the session from the home address of the MN, when attached to its home network, to a care-of-address after the MN roams to the foreign network.

On Page 8, line 11:

As is conventional with the internet protocol, nodes which communicate internet packets between each other provide the destination address as well as the source address in the basic internet packet header. Figure 2 provides an illustration of a route optimisation process between a correspondent node CN attached to a GPRS network and a mobile node MN. In Figure 2 the correspondent node CN is communicating internet packets to and from the mobile node MN whilst the correspondent ~~network MN node CN~~ is affiliated with a GPRS/UMTS network 200. As illustrated by two positions of the mobile node MN 202,204, the mobile node which was originally communicating internet packets with the correspondent network CN via its home network 210 moves to a foreign network 212. Thus originally the mobile -node MN was communicating internet packets via its home agent HA. When the mobile node MN moves from the home network 210 at position 202 to a foreign network 212 at position 204 internet packets according to a conventional operation of Ipv4 would have to be routed via the home agent. That is to say the destination address for packets sent to the mobile node MN would be its home address, and the source address of packets sent from the mobile node MN would be its home address. As such, internet packets would have to be routed via the foreign network 212 and the home network 210 to and from the correspondent node CN via the GPRS/UMTS network 200. It

will be appreciated that routing packets via the home agent after the mobile node MN has roamed to the foreign network consumes network resources unnecessarily and further increases the delay in communication of the internet packets.

On Page 10, lines 14-19:

As will be appreciated in the up-link direction, that is from the correspondent node CN 406 to the GGSN, corresponding tunnelling is employed to route the Internet packets back to the GGSN so that the internet packet can egress from the GPRS/UMTS network 200 to the foreign network 212. As shown in Figure [[2]] 4 a communication path from the MN to the GGSN 400 includes several routers 420,422, [[426]] 424 within the foreign network 212.

On Page 10, lines 21-22:

Also included within the GPRS/UMTS elements shown in Figure 4 in the GGSN 400 is a Traffic Flow Template (TFT) controller 470 and a Service Based Local Policy (SBLP) controller 472. The TFT 470 and the SBLP 472 operate in accordance with an embodiment of the present invention as will be described shortly to manage the communication of IP data packets from the GGSN to the mobile UE (CN) and from the mobile UE (CN) to the GGSN and outward to the foreign network 212.

On Page 11, line 5:

As shown in Figure 5 the TFT controller [[500]] 470 which operates in the GGSN mobile IP layer is provided with a list of source addresses 502 which are used to control the communication of IP data packets in accordance with a source address included within the Internet packet header. The TFT 500 arranges to communicate the IP data packets via an appropriate bearer which has been set up using the packet data protocol context activation which may be initiated by an application in the UE (CN), or on the mobile node MN and is analogous to logging onto a required destination.

On Page 11, line 12:

To select an appropriate UMTS bearer the GGSN has to establish a traffic flow template in accordance with the following parameters :

On Page 14, line 19:

One example of the information for the GGSN which may be provided in the field [[626]] 628 is the mobile node's home address. This provides a 128-bit address field. The router alert field in contrast is only 3-bits with the "hop-by-hop option type" field being only 5-bits. As a result, since every router along the communications path must only read 3-bits to determine whether the information is relevant to the router concerned, a performance loss is substantially reduced with respect to a performance loss which may have occurred if a remaining 128-bit address field was also required to be read by every router along the communications path.

On Page 14, lines 27-28:

In summary, by analysing the hop-by-hop Value field 626 in combination with the source address field 628 the TFT controller 500 can identify the appropriate bearer 520 to communicate the Internet packets to the correspondent node CN because the list 502 includes the home address of the mobile node. The operation of the GGSN when receiving IP packets for ingress to the packet radio network is summarised by the flow diagram of Figure 7 and explained as follows: SI : An internet packet according to the example in Figure 6 is received from the external network.

On Page 15, line 16:

S6: At step S6 the GGSN continues processing with either other functions, the processing of the current packet may however continue depending on the content of the GGSN information field.

On Page 16, line 13:

As will be appreciated, routers along a communications path between the mobile node and the correspondent node may now operate according to the standard, without being required to read the entire hop-by-hop extension header. This is because the router only needs to read as far as the router alert option field [[an]] and can ignore the remainder to the hop-by-hop extension header.